| | |
|---|---|
| 氏　　名 | EI MON CHO |
| 博士の専攻分野の名称 | 博士（学術） |
| 学位記号番号 | 博理工甲第 1087 号 |
| 学位授与年月日 | 平成 30 年 3 月 23 日 |
| 学位授与の条件 | 学位規則第 4 条第 1 項該当 |
| 学位論文題目 | Secure Multiple Group Data Deduplication in Cloud Data Storage（クラウドストレージにおける多重グループデータの安全な重複除外について） |
| 論文審査委員 | 委員長　教　授　重原　孝臣 |
| | 委　員　教　授　大澤　　裕 |
| | 委　員　教　授　内田　淳史 |
| | 委　員　准教授　吉浦　紀晃 |
| | 委　員　早稲田大学教育・総合科学学術院教授 |
| | 小柴　健史 |

## 論文の内容の要旨

Increasing the volume of redundant data by multiple clients in cloud storage becomes a vital challenge. Multiple group setting schemes have recently become important for enabling deduplication for a cloud server. We construct multiple-groups' schemes that allow one or more groups to subsequently upload or edit a file such that the cloud server can avoid duplicate according to the ownership of users. Cloud services become popular with a growing number of users, the demand for cloud storage information increases. One of the significant challenges of the cloud storage service is the management of increasing volume of data.

Deduplication removes these extra copies by saving only one copy of the redundant data and replacing the other copies with pointers to the original. Cloud data deduplication is used for eliminating the duplicate copies on the cloud storage providers. For example, the same file may be stored in several different places according to different users, or two or more files that are not identical may still consist of much of the same data.

Secure deduplication in cloud storage system becomes popular for both research and industrial communities. Most of the cloud computing environments (e.g., Amazon, Dropbox, Google Drive) try to reduce the cost of storage.

The motivation behind our thesis is to allow cross-groups for the file level deduplication which are controlled by each group manager. In this thesis, not only multiple users but also subsequent multiple groups may own a single file which is located in the same data storage. From the point of security and privacy views, various issues come up through the client-side deduplication. The deduplication can be done on a single user side, where the redundancy among his/her data is identified and removed, but the single user data deduplication is not very practical and does not yield maximum space saving. In this thesis, we have addressed the issue of the security of the data in the cloud storages when data deduplication is being in the cross-group user setting.

We first introduce three frameworks with the cross-group setting which can protect against duplication faking attacks and defend from the unpredictable data attacks. DDUP-MUG fits the original framework of deterministic MLE while

satisfying multiple group features by adding signature scheme. Generally, DDUP-MUG composed of three protocols: UPL-Dup protocol, EDT-Dup protocol, and DEL-Dup protocol. Moreover, DDUP-MUG reduces the bandwidth by sending only tag and signature pair while checking verification and duplication. DDUP-MUG ensures both the message security, tag consistency and the bandwidth efficiency among the cross group. DDUP-MUG supports extended demands that arise in realistic and secure scenarios.

Second, we proposed a new primitive group signcryption for deduplication called verifiable hash convergent group signcryption VHCGS by adding the properties of group signcryption and the verification facilities for the storage server (third party). We have designed a scheme that supports secure deduplication where several groups are sharing data by using VHCGS. This is an attempt to try out cross-group user deduplication in a real Big Data management. In doing so, we are taking the utility of existing schemes rather than proposing an entirely new one. We introduce a framework for a group signcryption scheme which can protect against duplication for the cloud providers and defend against unpredictable data attacks. VHCGS fits the original framework of deterministic hash convergent encryption while satisfying a group feature by adding the cloud server verifiable group signcryption. VHCGS is composed of three protocols: a setup protocol, an upload protocol, and a download protocol. VHCGS ensures message security and tag consistency as well as the bandwidth efficiency of the group user and cloud storage server. VHCGS supports the extended demands that arise in realistic and secure scenarios.

Finally, we proof the security of third party proxy re-encryption for group membership and non-group membership scheme. The main challenges were to make our schemes applicable in a real world scenario. For examples, there are three software developing companies allocated in different countries. There three companies are a kind of co-operation and they are trying to share a storage server. In this case, same redundant files owned by the different groups (companies) are one of the issues for cloud service provider. Firstly the storage server needs one administrator to remove the redundant file. Secondly, each company needs an agreement with the company before submitting every file or editing every file. By adding our cross-group deduplicaiton scheme to an existing storage server, the above two problems will be solved.

# 論文の審査結果の要旨

学位論文審査委員会は、平成 30 年 2 月 16 日に論文発表会を開催し、論文内容の発表に続いて詳細な質疑と論文内容の審査を行った。以下に審査結果を要約する。

クラウド容量サービスが一般的になり、その効率化運用が急務の課題となっている。同一ファイルがクラウド上に複数存在することは資源の有効利用の観点から望ましくなく、重複除外と呼ばれる同一ファイルを削除する技術が知られている。一方で、クラウド容量サービスは個人の枠を超えて組織内・グループ内で情報共有する形で利用されることもある。その場合、暗号化技術などを利用してプライバシー保護を行うことが一般的である。クラウド容量サービスにおいてプライバシーと重複除外を両立させることは、ファイル内容を秘匿することとファイル内容が同一かを比較することを同時に行うことであり、安全な重複除外のメカニズムを実現することは容易なことではない。暗号技術の安全性解析は理論的に行われることが一般的であることもあり、最初の安全な重複除外は Message Locked Encryption と呼ばれ、2013 年に Bellare らによって理論的な結果として構築された。これ以降、安全な重複除外の構築方法を発展させる研究がなされているが、理論的な発展が主であり、クラウド容量サービスの実際的な利用環境などを考慮した応用研究はほとんどなされていない。

そこで本研究では、複数グループがクラウド容量サービスを利用するという一つの利用形態に着目し、その利用形態における安全な重複除外のための技術を開発することを目的とする。一般の暗号技術においてもグループ利用を前提とした技術が存在するので、それらの基本性質を調査検討し、安全な重複除外のための技術と融合できるかを調査する。

第 1 章では、本論文の問題背景、安全な重複除外のための基本技術（Message Locked Encryption など）の説明、本論文で取り扱う多重グループという利用形態での重複除外技術の重要性、本論文の構成について述べている。

第 2 章では、暗号要素技術（公開鍵暗号、ハッシュ関数、電子署名、グループ署名、サインクリプション (signcryption)）の説明、暗号要素技術の安全性概念の定義を述べている。

第 3 章では、クラウド計算技術に関するセキュリティ問題に対して暗号技術がどのように貢献しているかを分類整理している。

第 4 章では、クラウド容量において、安全な重複除外を実現するために克服すべき問題を委細に検討している。重複除外というタスクを実際に行う実体がサーバであるのかユーザであるのかで生じる問題を類別し、それぞれにおいて安全な重複除外を実現するためのシステム設計方法を検討している。

第 5 章では、グループ署名と呼ばれる暗号技術を用いて、安全な重複除外メカニズムを実現する方法について新しい提案を行っている。グループ署名はグループの成員ならば誰でも文書に対して署名を付加する技術であり、しかも、グループの成員の誰かが署名したという事実は検証できるが、誰が署名したのかという個人の特定まではできない匿名性という性質を持っている。グループ署名を用いて安全な重複除外メカニズムを設計するためには、どのようにファイル管理を行うべきかというポリシーを Message Locked Encryption をベースに策定し、そのポリシーを実現させるためのシステム設計方法を提案している。具体的には、ファイルをクラウド容量に初めて預託する場合、ファイルを更新する場合、ファイルを削除する場合に分けて、それぞれを実現するためのプロトコルを提案している。さらに、暗号学的な安全性解析を行うことで安全性が達成されていることを示している。

第 6 章では、単純な形式のグループサインクリプションと代理人サインクリプションと呼ばれる既存の暗

号スキームを融合させて、重複除外に適した形式、Hash convergent グループサインクリプションという暗号スキームを新たに提案し、それを実現する方法を示している。サインクリプションは公開鍵暗号と電子署名を同時に行う暗号スキームであるが、公開鍵暗号機能と電子署名機能が不可分な形で実現されており、その不可分性によりある種の攻撃可能性を排除することにつながっている。Message Locked Encryption の代わりに、検証可能 Hash Convergent グループ署名というスキームを構築し、これを用いて第５章で定めたポリシーを実現するためのシステム設計方法を提案している。また、ファイル預託・ファイル抽出のためのプロトコルを提案している。ここでの提案は汎用性が高く、モバイルデータ転送、とくに、SMS (Short Message Service) に適用可能であることを例証している。

第５章および第６章で提案した重複除外はファイル預託・更新・抽出・削除の基本４機能がすべて同時に実現されていないという問題があり、一つの重複除外システムで基本４機能がすべて実現されているような完全な重複除外システムが望ましい。第７章では、完全な重複除外システムの実現に向けて、必要になると思われる暗号要素技術として、複数グループのための非転送型代理人再暗号化方式を構成している。

最後に第８章では、本論文で得られた成果をまとめている。とくに、第５章および第６章で提案した新方式について長所・短所をまとめているとともに、今後の課題を述べている。

以上、要するに、本論文では、クラウド容量の多重グループという利用形態の重要性を説明し、それを可能にする安全な重複除外メカニズムを提案することに成功している。本研究で得られた知見は、安全なクラウド容量の設計において重要な意義があると考えられる。また、現実にサービスが提供されている商用クラウド容量に対しても適用可能であり、応用上でも有用と期待できる。

本論文の主な内容は、査読付き学術雑誌論文３編（数理電子情報コースにおいて学術雑誌論文相当と見なす査読付き国際会議論文を含む）で公表ないしは受理されている。

以上を総合し、本学位論文審査委員会は、本論文が、博士（学術）の学位を授与するに十分に値するものと認め、「合格」と判定した。